

# Sequential discrimination of qudits by multiple observers

Mark Hillery<sup>1,2</sup> and Jihane Mimih<sup>3</sup>

<sup>1</sup>*Department of Physics, Hunter College of the City University of New York, 695 Park Avenue, New York, NY 10065 USA*

<sup>2</sup>*Physics Program, Graduate Center of the City University of New York, 365 Fifth Avenue, New York, NY 10016*

<sup>3</sup>*Naval Air Warfare Center Aircraft Division, Patuxent River, MD 20670 USA*

We discuss a scheme in which sequential state-discrimination measurements are performed on qudits to determine the quantum state in which they were initially prepared. The qudits belong to a set of nonorthogonal quantum states and hence cannot be distinguished with certainty. Unambiguous state discrimination allows error-free measurements at the expense of occasionally failing to give a conclusive answer about the state of the qudit. Qudits have the potential to carry more information per transmission than qubits. We considered the situation in which Alice sends one of  $N$  qudits, where the dimension of the qudits is also  $N$ . We looked at two cases, one in which the states all have the same overlap and one in which the qudits are divided into two sets, with qudits in different sets having different overlaps. We also studied the robustness of our scheme against a simple eavesdropping attack and found that by using qudits rather than qubits, there is a greater probability that an eavesdropper will introduce errors and be detected.

PACS numbers: 03.65.Yz, 03.67.Hk

## I. INTRODUCTION

It is often thought that measuring a quantum mechanical system again after it has been already measured does not yield useful information. The first measurement places the system in an eigenstate of the observable that was measured, and a second measurement would only see this eigenstate and not the original state. This is too narrow a view for several reasons. First, the spectral resolution of the observable may not consist of rank-one projections, so that the same measurement result can lead to different post-measurement states. This can also be true if the measurement is described by a POVM (positive-operator-valued measure) instead of projection operators, i.e. there is not a one-to-one correspondence between the measurement result and the post-measurement state. Even in the case of when each measurement result yields a unique output state, it is possible for a second measurement to learn something about the initial state of the system [1].

In an earlier paper, we studied a particular example of sequential measurements on a single system [2]. A qubit in one of two states was prepared by Alice and then sent to Bob, who performed an unambiguous state discrimination measurement on it, after which Bob sent the qubit on to Charlie, who also performed an unambiguous state discrimination measurement on it. States that are not orthogonal cannot be discriminated perfectly, and in unambiguous discrimination, while we will never make an error, the measurement can sometimes fail [3–5]. In the sequential scenario, there is a non-zero probability that both Bob’s and Charlie’s measurements succeed, so that they are both able to identify the state Alice sent. In this case Alice is able to send a bit to both Bob and Charlie using only a single qubit.

In this paper we would like to extend this scenario to higher dimensional systems, qudits, and see what effect using qudits instead of qubits has on failure probabilities

and on the amount of information that can be transmitted. In particular, Alice will send one of  $N$  qudits to Bob, where the dimension of the qudits is also  $N$ . We will look at two cases. In the first, the qudit states have the property that the overlap between any two of them is the same. In the second, the qudits are divided into two sets, and there are three possible overlaps. Any two qudits in the same set have the same overlap, though the overlaps can be different for the two sets. Any two qudits from different sets have the same overlap, and that overlap will, in general, be different from the ones for qudits in the same set. Using states with different overlaps could complicate the task of someone trying to obtain information about the transmissions. In both cases, Bob will apply an unambiguous discrimination measurement to the qudit, and then send it on to Charlie. One might think that sending one of  $N$  possible qudits rather than one of two qubits might have an adverse effect on the failure probability, but we find that it does not. Consequently, using qudits allows more information to be sent per transmission, and we will examine the channel capacity of this system. We will also see what happens if an additional party attempts to extract information about the qudit state by using a minimum-error measurement and determine how the information thereby gained about the transmitted state depends on dimension. These issues become important if this protocol is to be used for communication purposes.

## II. EQUAL OVERLAPS

### A. Qudit states with equal overlap

Consider  $N$  states in an  $N$ -dimensional space,  $|\eta_j\rangle$ ,  $j = 1, 2, \dots, N$ , with the property that  $\langle \eta_j | \eta_k \rangle = s$  for  $j \neq k$ , and we shall assume that  $s$  is real. An example of such a set would be the  $N$ -qubit states

$|\eta_j\rangle = |0\rangle^{\otimes(j-1)}|\mu\rangle|0\rangle^{\otimes(N-j)}$ . Here,  $|\mu\rangle = \alpha|0\rangle + \beta|1\rangle$ , and  $s = |\alpha|^2$ . A second example is given by the following. Let  $\{|j\rangle | j = 1, 2, \dots, N\}$  be an orthonormal basis and let

$$|\eta_j\rangle = \frac{1}{[(N-1)|\alpha|^2 + |\beta|^2]^{1/2}} \left( \beta|j\rangle + \alpha \sum_{k=1, k \neq j}^N |k\rangle \right). \quad (1)$$

In this case we have that

$$s = 1 - \frac{|\alpha - \beta|^2}{(N-1)|\alpha|^2 + |\beta|^2}. \quad (2)$$

We will assume that Alice sends one of these states, with each state being equally likely, to a second party, who then measures the state and then sends the resulting state on to the next party, who then also measures the state. This procedure can be repeated, with each party measuring the state they receive and sending the post-measurement state on to the next party, until the qudit reaches the last party, who simply measures it.

In order to implement the procedure in the previous paragraph, we first need to find an unambiguous discrimination measurement to distinguish the states  $\{|\eta_j\rangle | j = 1, 2, \dots, N\}$ . Unambiguous discrimination for symmetric states, of which the case of equal overlaps is an example, was studied by Chefles and Barnett [7], and the equal-overlap case was studied in detail by Englert and Řehaček [8]. Because we will need the details of the equal-overlap case in order to examine sequential measurements, we will derive this case from the beginning. In addition, the method we use can be extended to the case when the overlaps are not equal. The measurement operators,  $\Pi_j$ , for  $j = 0, 1, \dots, N$ , which are positive, satisfy  $\langle \eta_j | \Pi_k | \eta_j \rangle = 0$  for  $j, k = 1, 2, \dots, N$  and  $j \neq k$ , and  $\sum_{j=0}^N \Pi_j = I$ . The operator  $\Pi_j$ ,  $j = 1, 2, \dots, N$ , corresponds to the detection of the state  $|\eta_j\rangle$ , and  $\Pi_0$  corresponds to the measurement failing. If we are given  $|\eta_j\rangle$ , the probability of properly identifying it is  $\langle \eta_j | \Pi_j | \eta_j \rangle$ . Because of the condition  $\langle \eta_j | \Pi_k | \eta_j \rangle = 0$ , for  $1 \leq j, k \leq N$  and  $k \neq j$ , we will never make a mistake, that is claim we found  $|\eta_k\rangle$  when  $|\eta_j\rangle$  was sent. On the other hand, the measurement can fail, and this happens with a probability of  $\langle \eta_j | \Pi_0 | \eta_j \rangle$ . Clearly we have that

$$\Pi_j = c_j |\eta_j^\perp\rangle \langle \eta_j^\perp| \quad (3)$$

where  $c_j$  is a constant and  $|\eta_j^\perp\rangle$  is the vector in the space that satisfies  $\langle \eta_k | \eta_j^\perp \rangle = 0$  for  $k \neq j$ . We will assume that all of the  $c_j$ 's are the same, that is,  $c_j = c$ .

The first thing to do is to find  $|\eta_j^\perp\rangle$ . We can expand it in terms of the vectors  $|\eta_j\rangle$ ,

$$|\eta_j^\perp\rangle = \sum_{k=1}^N d_k |\eta_k\rangle. \quad (4)$$

The condition  $\langle \eta_n | \eta_j^\perp \rangle = 0$  for  $n \neq j$  gives us

$$d_n = - \sum_{k \neq n} s d_k. \quad (5)$$

Setting  $\Lambda = \sum_{k=1}^N d_k$ , this can be expressed as

$$d_n = \frac{-s}{1-s} \Lambda \quad (6)$$

for  $n \neq j$ . Inserting this expression into the definition of  $\Lambda$  we find that

$$\Lambda = d_j - (N-1)\Lambda \frac{s}{1-s}, \quad (7)$$

or

$$\Lambda = \frac{1-s}{1+s(N-2)} d_j. \quad (8)$$

This implies that for  $k \neq j$

$$d_k = \frac{-s}{1+s(N-2)} d_j \quad (9)$$

and

$$|\eta_j^\perp\rangle = d_j |\eta_j\rangle - \frac{s}{1+s(N-2)} d_j \sum_{k=1, k \neq j}^N |\eta_k\rangle. \quad (10)$$

One can find  $d_j$  by normalizing the state to one, which gives

$$d_j = \left\{ \frac{1+s(N-2)}{(1-s)[1+(N-1)s]} \right\}^{1/2} \quad (11)$$

and this then implies that

$$\langle \eta_j | \eta_j^\perp \rangle = \left\{ \frac{(1-s)[1+(N-1)s]}{1+s(N-2)} \right\}^{1/2} \quad (12)$$

The next step is to find the range of  $c$  that leaves  $\Pi_0 = I - \sum_{j=1}^N \Pi_j$  positive. If we express an arbitrary vector  $|\psi\rangle$  as

$$|\psi\rangle = \sum_{j=1}^N \alpha_j |\eta_j\rangle, \quad (13)$$

the condition that  $\langle \psi | (I - \sum_{j=1}^N \Pi_j) | \psi \rangle \geq 0$  can be expressed as

$$\sum_{j,k=1}^N \alpha_j^* \tilde{M}_{jk} \alpha_k \geq 0, \quad (14)$$

where  $\tilde{M}_{jj} = q$ ,  $\tilde{M}_{jk} = s$  for  $j \neq k$ , and

$$q = 1 - c \frac{(1-s)[1+(N-1)s]}{1+(N-2)s}. \quad (15)$$

We now need to find the condition on  $q$  so that  $\tilde{M}$  has only non-negative eigenvalues. Let the column vector  $(x_1, x_2, \dots, x_N)^T$  be an eigenvector of  $\tilde{M}$  with eigenvalue  $\lambda$ . Then the eigenvalue equation for  $\tilde{M}$  becomes

$$q x_j + s \sum_{k \neq j} x_k = \lambda x_j, \quad (16)$$

for  $j = 1, 2, \dots, N$ . Setting  $\xi = \sum_{j=1}^N x_j$ , we find that

$$(\lambda - q + s)x_j = s\xi. \quad (17)$$

If we now sum both sides of this equation over  $j$ , we obtain the consistency condition

$$(\lambda - q + s)\xi = Ns\xi. \quad (18)$$

There are now two possibilities. If  $\xi \neq 0$ , then  $\lambda = (N-1)s + q$ . If  $\xi = 0$ , then we must have  $\lambda = q - s$  if at least one of the  $x_j$  is to be nonzero. For  $\tilde{M}$  to be non-negative we need both eigenvalues to be non-negative, and this condition will be fulfilled if  $q \geq s$ , which implies

$$c \leq \frac{1 + s(N-2)}{1 + s(N-1)}. \quad (19)$$

We can relate this condition to the overall failure probability. If each of the  $|\eta_j\rangle$  are equally likely, we can define the success probability of the measurement to be

$$p = \frac{1}{N} \sum_{j=1}^N \langle \eta_j | \Pi_j | \eta_j \rangle = 1 - q, \quad (20)$$

where the last equality follows from Eqs. (3) and (12). This implies that  $q = 1 - p$  is just the failure probability of the measurement.

### B. Unambiguous state discrimination using consecutive measurements

In the previous section, we have shown that the failure probability to distinguish between  $N$  qudit states cannot be lower than the overlap of the states when making an optimum single measurement. Here, we want to extend this scheme to allow for consecutive measurements. In this scenario, Alice prepares a qudit in a quantum state belonging to the set  $\{|\eta_1\rangle, |\eta_2\rangle, \dots, |\eta_N\rangle\}$  and sends it to Bob. Bob performs unambiguous state discrimination on the qudit he receives and sends it on to the next party. Each party performs unambiguous state discrimination on the qudit he or she receives and sends it to the next party until all  $N$  parties get the qudit and perform measurements on it. This should be done in such a way that each party has a nonzero probability of correctly identifying the state of the qudit. The idea here is that each party, except the last, performs a non-optimal measurement on its qudit so that some information about the quantum state is left after it has been measured. The last party, of course, can perform an optimal measurement in order to extract all of the remaining information. The probability that Bob unambiguously detects the state  $|\eta_k\rangle$  sent by Alice is given by

$$p_k = \langle \eta_k | \Pi_k^B | \eta_k \rangle = c |\langle \eta_k | \eta_k^\perp \rangle|^2 \quad (21)$$

We need to determine the state after Bob performs his measurement since it will become the input state for the

next party's, Charlie's, measurement. This state can be expressed in terms of the detection operators  $A_k$  which are related to the measurement operators  $\Pi_k^B$  by

$$\Pi_k^B = A_k^\dagger A_k = c |\eta_k^\perp\rangle \langle \eta_k^\perp|, \quad (22)$$

for  $k = 1, 2, \dots, N$ . When Bob's measurement succeeds, his post-measurement state is:

$$|\phi_k\rangle = \frac{A_k |\eta_k\rangle}{\|A_k |\eta_k\rangle\|}, \quad (23)$$

and if Bob's measurement yields an inconclusive result, the post-measurement state is:

$$|\chi_k\rangle = \frac{A_0 |\eta_k\rangle}{\|A_0 |\eta_k\rangle\|}. \quad (24)$$

Since the only requirement on  $A_k$  is  $A_k^\dagger A_k = c_k |\eta_k^\perp\rangle \langle \eta_k^\perp|$ , we have considerable freedom in choosing the detection operators  $A_k$ . We shall choose

$$A_k = \sqrt{c} |\phi_k\rangle \langle \eta_k^\perp|, \quad (25)$$

where the states  $|\phi_j\rangle$  satisfy  $\langle \phi_j | \phi_k \rangle = t$ , for  $j \neq k$  and  $t$  real. Now when Bob's measurement succeeds, he will send a qudit in the state  $|\phi_k\rangle$  to Charlie, and if the measurement fails, he will send a qudit in the state  $|\chi_k\rangle$  to Charlie. For Charlie to be able to use unambiguous state discrimination, the states he wishes to distinguish need to be linearly independent [9]. Since we are in an  $N$ -dimensional Hilbert space, it is necessary to have  $|\chi_k\rangle = |\phi_k\rangle$ . We can therefore express  $A_0$  as

$$A_0 = \sum_k a_k |\phi_k\rangle \langle \eta_k^\perp|, \quad (26)$$

where the  $a_k$  are constants that need to be determined. We then have

$$\begin{aligned} \langle \eta_k | A_0^\dagger A_0 | \eta_k \rangle &= |a_k|^2 r = q_k \\ \langle \eta_k | A_0^\dagger A_0 | \eta_m \rangle &= a_m a_k^* r t, \end{aligned} \quad (27)$$

where  $r = |\langle \eta_j | \eta_j^\perp \rangle|^2$  and  $q_k$  is the failure probability to identify the state  $|\eta_k\rangle$ . Due to the symmetry of the problem, we shall choose all of the coefficients  $a_k$  to be the same, that is  $a_k = a$  for  $k = 1, 2, \dots, N$ , which implies that the failure probability for each of the states is the same, that is  $q_k = r|a|^2 = q$ . The operator  $A_0^\dagger A_0$  can now be expressed in a matrix form in the basis  $\{|\eta_k\rangle | k = 1, 2, \dots, N\}$  as

$$A_0^\dagger A_0 = \begin{pmatrix} q & qt & \cdots & qt \\ qt & q & \cdots & qt \\ \vdots & \vdots & \ddots & \vdots \\ qt & qt & \cdots & q \end{pmatrix} \quad (28)$$

The operator  $A_0^\dagger A_0$  can also be written as  $A_0^\dagger A_0 = I - c \sum_k |\eta_k^\perp\rangle \langle \eta_k^\perp|$ , which in matrix form can be expressed as

$$A_0^\dagger A_0 = \begin{pmatrix} 1 - cr & s & \cdots & s \\ s & 1 - cr & \cdots & s \\ \vdots & \vdots & \ddots & \vdots \\ s & s & \cdots & 1 - cr \end{pmatrix} \quad (29)$$

Comparing the two different expressions for the failure operator  $A_0^\dagger A_0$  in Eqs. (28) and (29), we see that they will be consistent if  $q = \frac{s}{t}$  and  $q = 1 - cr$ . The second condition already follows from the Eqs. (12) and (15). The first condition and the condition  $q \geq s$  from section II imply that  $t \geq s$ .

Let us now summarize the situation, and for the moment, assume that the only actors are Alice, Bob and Charlie. Alice sends one of the states  $\{|\eta_j\rangle | j = 1, 2, \dots, N\}$ , say  $|\eta_k\rangle$ , to Bob. Bob then measures the state. Whether his measurement succeeds or fails, it is so designed that he sends the state  $|\phi_k\rangle$  on to Charlie. Note that since  $t \geq s$ , the states Charlie receives are, in general, less distinguishable than those in Alice's original set. This is because Bob's measurement has extracted some information from the state. Charlie then performs an optimal unambiguous measurement on the states  $\{|\phi_j\rangle | j = 1, 2, \dots, N\}$ . Let us call Bob's failure probability  $q_B$  and Charlie's  $q_C$ . From our results we have that  $q_B \geq s$ ,  $q_C \geq t$ , and  $q_B = s/t$ , where  $t \geq s$ . Now if Charlie's measurement is optimal, he will have  $q_C = t$ , which then implies that  $q_B q_C = s$ . If we want Bob and Charlie to have equal failure probabilities, we will choose  $q_B = q_C = \sqrt{s}$ . This implies that the probability that both measurements succeed is  $(1 - \sqrt{s})^2$ . An identical result was found earlier for qubits [2]. This shows that there is a considerable advantage to using qudits. Since the probability for both measurements to succeed is the same for qubits and qudits, that is, it is independent of the dimension of the system, and more information can be sent using qudits, it is clearly advantageous to use higher dimensional systems.

Now let us extend the scheme to more actors. Instead of Alice, Bob, and Charlie, we will have Alice, Bob<sub>1</sub>, ... Bob<sub>M</sub>. Alice sends a qudit in the state  $|\eta_k\rangle$ , which belongs to a known set  $\{|\eta_1\rangle, \dots, |\eta_N\rangle\}$  to Bob<sub>1</sub>, who performs an unambiguous state discrimination measurement to extract information about the quantum state he received. The measurement succeeds with a probability  $1 - q_1$ , where  $q_1 \geq s$ , and it results in a state  $|\phi_k^{(1)}\rangle$ . The states  $\{|\phi_k^{(1)}\rangle | k = 1, 2, \dots, N\}$  have an overlap  $t^{(1)}$ , which exceeds the overlap of the initial states  $s$ , i.e.  $t^{(1)} \geq s$ . Bob<sub>1</sub> then sends the state  $|\phi_k^{(1)}\rangle$  on to Bob<sub>2</sub>. This continues until the qudit reaches Bob<sub>M</sub>. While Bob<sub>1</sub> through Bob<sub>M-1</sub> perform non-optimized measurements to extract information about the state, Bob<sub>M</sub> performs an optimized measurement to extract all the information remaining in the quantum state since the last post-measurement state does not need to carry any further information about the initial state. This implies that the overlap of the final set of post-measurement states,  $t^{(M)}$  will be 1. The probability that all of the measurements succeed is

$$p_{succ} = \prod_{l=1}^M (1 - q_l), \quad (30)$$

where  $q^{(l)}$  is the probability that the measurement made

by Bob<sub>l</sub> fails. The total success probability is just the success probability for each input state times the probability of the corresponding input state. Since, in our case, each state is equally likely and the success probability for each state is the same, the total success probability is the same as the success probability for each state, which is the result given in the above equation.

When Bob<sub>1</sub> makes a measurement on the state he receives from Alice, his failure probability to identify the state is  $q^{(1)} = s/t^{(1)}$  where  $s$  is the overlap of the initial states while  $t^{(1)}$  is the overlap of the post-measurement states. The failure probability associated with the second measurement must satisfy a similar constraint that can be obtained by replacing  $s$  by the overlap of the new input states  $t^{(1)}$  and  $t^{(1)}$  by  $t^{(2)}$ , the overlap of the post-measurement states resulting from the second measurement. The final measurement is characterized by the fact that the overlap between the post-measurement states is one since the measurement is optimum at this stage, which results in  $q^{(M)} = t^{(M-1)}$ . These constraints can be summarized in the following equations:

$$\begin{aligned} q^{(1)} &= s/t^{(1)} \\ q^{(2)} &= t^{(1)}/t^{(2)} \\ &\vdots \\ q^{(M)} &= t^{(M-1)}/t^{(M)} = t^{(M-1)} \end{aligned} \quad (31)$$

If we assume for simplicity that  $q^{(1)} = q^{(2)} = \dots = q^{(M)} = w$ , we find that  $w = s^{\frac{1}{M}}$ . The success probability is then given by

$$p_{succ} = (1 - s^{\frac{1}{M}})^M \quad (32)$$

### III. QUDIT STATES WITH DIFFERENT OVERLAPS

Now let us consider  $N$   $N$ -qubit states of the form

$$|\eta_j\rangle = \begin{cases} |0\rangle^{\otimes(j-1)} |\mu_1\rangle |0\rangle^{\otimes(N-j)} & 1 \leq j \leq M \\ |0\rangle^{\otimes(j-1)} |\mu_2\rangle |0\rangle^{\otimes(N-j)} & M+1 \leq j \leq N \end{cases} \quad (33)$$

Suppose that  $\langle 0|\mu_1\rangle = s_1 > 0$  and  $\langle 0|\mu_2\rangle = s_2 > 0$ . The collection of states  $\{|\eta_j\rangle | j = 1, 2, \dots, N\}$  now has the property that  $\langle \eta_j | \eta_k \rangle$  is equal to  $s_1^2$  for  $j, k \leq M$ ,  $s_2^2$  for  $j, k \geq M+1$ , and  $s_1 s_2$  for either  $j \leq M$  and  $k \geq M+1$  or  $j \geq M+1$  and  $k \leq M$ .

The first thing we need to do to unambiguously discriminate the states  $|\eta_j\rangle$  is to find the states  $|\eta_j^\perp\rangle$ , as we did in the case of equal overlaps. Because the details of the calculation are similar to those of the equal-overlap case, we present them, and explicit expressions for the vectors  $|\eta_j^\perp\rangle$ , in an appendix. What we will need here are the quantities  $\Gamma_1$ , which is equal to  $|\langle \eta_j | \eta_j^\perp \rangle|^2$  for  $j \leq M$ ,

$$\Gamma_1 = \frac{1}{D_1} [(1 - s_1^2)(D_1 + s_1^2(1 - s_2^2))], \quad (34)$$

and  $\Gamma_2$ , which is equal to  $|\langle \eta_j | \eta_j^\perp \rangle|^2$  for  $j \geq M+1$ ,

$$\Gamma_2 = \frac{1}{D_2} [(1 - s_2^2)(D_2 + s_2^2(1 - s_1^2))]. \quad (35)$$

See the appendix for explicit expressions for  $D_1$  and  $D_2$ . For the POVM elements we choose

$$\begin{aligned} \Pi_j &= c_1 |\eta_j^\perp\rangle \langle \eta_j^\perp| & j \leq M \\ \Pi_j &= c_2 |\eta_j^\perp\rangle \langle \eta_j^\perp| & j \geq M+1, \end{aligned} \quad (36)$$

and  $\Pi_0 = I - \sum_{j=1}^N \Pi_j$ . The positivity condition that  $\langle \psi | \Pi_0 | \psi \rangle \geq 0$  becomes (see Eqs. (13) and (14))

$$\sum_{j,k=1}^N \alpha_j^* \tilde{L}_{jk} \alpha_k \geq 0, \quad (37)$$

where  $\tilde{L}_{jj} = 1 - c_1 \Gamma_1$  for  $j \leq M$ ,  $\tilde{L}_{jj} = 1 - c_2 \Gamma_2$  for  $j \geq M+1$ ,  $\tilde{L}_{jk} = s_1^2$  for  $j, k \leq M$  and  $j \neq k$ ,  $\tilde{L}_{jk} = s_2^2$  for  $j, k \geq M+1$  and  $j \neq k$ , and finally  $\tilde{L}_{jk} = s_1 s_2$  for  $j \leq M$  and  $k \geq M+1$  or  $j \geq M+1$  and  $k \leq M$ .

In order to show that  $\tilde{L}$  is positive, we need to find its eigenvalues. As before, letting the eigenvector of  $\tilde{L}$  be the column vector  $(x_1, x_2, \dots, x_N)^T$ , the eigenvalue equations are for  $j \leq M$

$$(1 - \Gamma_1 c_1) x_j + s_1^2 \sum_{k=1, k \neq j}^M x_k + s_1 s_2 \sum_{k=M+1}^N x_k = \lambda x_j, \quad (38)$$

and for  $k \geq M+1$

$$s_1 s_2 \sum_{k=1}^M x_k + (1 - \Gamma_2 c_2) x_j + \sum_{k=M+1, k \neq j}^N s_2^2 x_k = \lambda x_j. \quad (39)$$

Setting

$$\xi_1 = \sum_{k=1}^M x_k \quad \xi_2 = \sum_{k=M+1}^N x_k, \quad (40)$$

and summing the first of the above equations from  $j = 1$  to  $M$  and the second from  $j = M+1$  to  $N$ , we find

$$\begin{aligned} 0 &= [(M-1)s_1^2 - \lambda + 1 - \Gamma_1 c_1] \xi_1 + M s_1 s_2 \xi_2 \\ 0 &= (N-M) s_1 s_2 \xi_1 \\ &\quad + [(N-M-1)s_2^2 - \lambda + 1 - \Gamma_2 c_2] \xi_2. \end{aligned} \quad (41)$$

These equations will have nonzero solutions for  $\xi_1$  and  $\xi_2$  if the determinant of the coefficients of the above equations vanishes. Setting

$$F_1 = 1 - \Gamma_1 c_1 - s_1^2 \quad F_2 = 1 - \Gamma_2 c_2 - s_2^2, \quad (42)$$

this condition becomes

$$\begin{aligned} 0 &= \lambda^2 - \lambda [M s_1^2 + (N-M) s_2^2 + F_1 + F_2] \\ &\quad + F_1 F_2 + M s_1^2 F_2 + (N-M) s_2^2 F_1. \end{aligned} \quad (43)$$

The solutions to this equation give us two of the eigenvalues of  $\tilde{L}$ , and they will be non-negative if

$$M s_1^2 F_2 + (N-M) s_2^2 F_1 + F_1 F_2 \geq 0. \quad (44)$$

The other eigenvalues come from the case  $\xi_1 = \xi_2 = 0$ . In that case the eigenvector equations become

$$(1 - \Gamma_1 c_1 - s_1^2 - \lambda) x_j = 0, \quad (45)$$

for  $j \leq M$  and

$$(1 - \Gamma_2 c_2 - s_2^2 - \lambda) x_j = 0, \quad (46)$$

for  $j \geq M+1$ . In order that not all of the  $x_j$  for  $j \leq M$  be equal to zero, we need  $\lambda = 1 - \Gamma_1 c_1 - s_1^2$ , and this and the condition  $\xi_1 = 0$  results in  $M-1$  eigenvectors. For not all of the  $x_j$  for  $j \geq M+1$  to be zero, we need  $\lambda = 1 - \Gamma_2 c_2 - s_2^2$ , and this and the condition  $\xi_2 = 0$  yields  $N-M-1$  eigenvectors. Therefore, our conditions for  $\tilde{L}$  to be non-negative are

$$1 - s_1^2 \geq \Gamma_1 c_1 \quad 1 - s_2^2 \geq \Gamma_2 c_2. \quad (47)$$

Note that these conditions are equivalent to  $F_1 \geq 0$  and  $F_2 \geq 0$ , so that if they are satisfied, so is the condition in Eq. (44).

Next we need to specify the post-measurement states and the detection operators. We want the state  $|\eta_j\rangle$  to go to the state  $|\phi_j\rangle$  after the measurement, where  $\langle \phi_j | \phi_k \rangle$  is equal to  $t_1^2$  for  $j, k \leq M$ ,  $t_2^2$  for  $j, k \geq M+1$ , and  $t_1 t_2$  for either  $j \leq M$  and  $k \geq M+1$  or  $j \geq M+1$  and  $k \leq M$ . This will be the case if we choose the detection operators to be

$$A_j = \begin{cases} \sqrt{c_1} |\phi_j\rangle \langle \eta_j^\perp| & 1 \leq j \leq M \\ \sqrt{c_2} |\phi_j\rangle \langle \eta_j^\perp| & M+1 \leq j \leq N, \end{cases} \quad (48)$$

and

$$A_0 = a_1 \sum_{j=1}^M |\phi_j\rangle \langle \eta_j^\perp| + a_2 \sum_{j=M+1}^N |\phi_j\rangle \langle \eta_j^\perp|, \quad (49)$$

with  $a_1$  and  $a_2$  to be determined. Defining  $q_1 = 1 - c_1 \Gamma_1$ , which is the failure probability for the states  $|\eta_j\rangle$ ,  $1 \leq j \leq M$ , and  $q_2 = 1 - c_2 \Gamma_2$ , which is the failure probability for  $|\eta_j\rangle$ ,  $M+1 \leq j \leq N$ , and setting  $A_0^\dagger A_0$  equal to  $I - \sum_{j=1}^N \Pi_j$ , we find that

$$\begin{aligned} q_1 &= a_1^2 \Gamma_1 = \frac{s_1^2}{t_1^2} \\ q_2 &= a_2^2 \Gamma_2 = \frac{s_2^2}{t_2^2} \\ s_1 s_2 &= a_1 a_2 t_1 t_2 \sqrt{\Gamma_1 \Gamma_2} = \sqrt{q_1 q_2} t_1 t_2. \end{aligned} \quad (50)$$

Note that the condition in the last line is consistent with the two in the first two lines. Also note that the positivity conditions in Eq. (47) can be stated as  $q_1 \geq s_1^2$  and  $q_2 \geq s_2^2$ .

Now let us look at the situation where Alice sends a qudit to Bob, who measures it, and then sends it on to Charlie, who also measures it. The failure probabilities for Bob's measurement are  $q_{1B} \geq s_1^2$  and  $q_{2B} \geq s_2^2$ , and those for Charlie's measurement are  $q_{1C} \geq t_1^2$  and  $q_{2C} \geq t_2^2$ . Charlie would perform an optimal unambiguous discrimination measurement, so we would have  $q_{1C} = t_1^2$  and  $q_{2C} = t_2^2$ . In this case the equations in the previous paragraph imply that  $q_{1B}q_{1C} = s_1^2$  and  $q_{2B}q_{2C} = s_2^2$ . In the case that Bob and Charlie have the same failure probabilities, we have  $q_{1B} = q_{1C} = s_1$  and  $q_{2B} = q_{2C} = s_2$ .

#### IV. CHANNEL CAPACITY

Let us begin with the simplest situation, just two actors, Alice and Bob, with Alice sending qubits in one of two nonorthogonal states to Bob. Using unambiguous discrimination, Bob either identifies the state with a probability  $p$ , or fails to do so with a probability  $q = 1 - p$ . This situation is described by a binary erasure channel. Alice sends a classical bit, which is either 0 or 1 to Bob, and Bob is able to read the bit with a probability  $p$ . This channel can be characterized by its channel capacity. The channel capacity for any discrete memoryless channel is defined to be the mutual information between the sender and receiver (in this case Alice and Bob) maximized over probability distributions of channel inputs. It is the maximum rate at which information can be sent through the channel [10]. The channel capacity for a binary erasure channel in which a fraction  $q$  of the bits are erased is just  $1 - q$ .

In order to determine how much of an advantage using qudits has over using qubits, we need to find the channel capacity of an erasure channel that has  $N$  possible inputs instead of two. Let the channel inputs be described by a random variable  $X$  and the outputs be described by a random variable  $Y$ . The possible inputs are  $\{x\}$ , which occur with probability  $P_{in}(x)$ , and the possible outputs are  $\{y\}$ , which occur with probability  $P_{out}(y)$ . The channel is characterized by a conditional probability,  $P(y|x)$ , which is the probability of detecting  $y$  at the output if the input was  $x$ . The mutual information between the input and the output,  $I(Y; X)$  is given by

$$I(Y; X) = H(Y) - H(Y|X), \quad (51)$$

where  $H(Y)$  is the Shannon information of  $Y$ ,

$$H(Y) = - \sum_y P_{out}(y) \log P_{out}(y), \quad (52)$$

and the conditional entropy is

$$H(Y|X) = - \sum_{x,y} P_{in}(x) P(y|x) \log P(y|x). \quad (53)$$

The logarithms here are base 2.

In our case, both the input set is  $\{1, 2, \dots, N\}$ , and the output set is  $\{1, 2, \dots, N, e\}$ , where  $e$  corresponds to the

case that the input is erased, or, in the quantum case, the failure of the measurement. We then have, for the equal overlap case,

$$P(y|x) = \begin{cases} (1 - q_e) & y = x \\ q_e & e \\ 0 & \text{otherwise,} \end{cases} \quad (54)$$

where  $q_e$  is the probability that the input is erased. This implies that

$$P_{out}(y) = \sum_x P(y|x) P_{in}(x) = \begin{cases} (1 - q_e) P_{in}(y) & y \neq e \\ q_e & y = e. \end{cases} \quad (55)$$

We now find that

$$\begin{aligned} H(Y|X) &= h(q_e) \\ H(Y) &= h(q_e) \\ &\quad - (1 - q_e) \sum_{y \neq e} P_{in}(y) \log P_{in}(y). \end{aligned} \quad (56)$$

where

$$h(q_e) = -q_e \log q_e - (1 - q_e) \log(1 - q_e). \quad (57)$$

Now the channel capacity,  $C$ , is

$$C = \max_{P_{in}} I(Y; X), \quad (58)$$

and the maximum of the second term in  $H(Y)$ , see Eq. (56), occurs when  $P_{in}(x) = 1/N$ . This gives us

$$C = (1 - q_e) \log N. \quad (59)$$

Therefore, the use of qudits rather than qubits results in a  $\log N$  improvement in the channel capacity, since for the Alice-Bob channel, we have  $q_e = s$ , independent of the dimension.

Now let us look at the Alice-Bob-Charlie case considered in Section II. The capacity of the Alice-Bob channel is  $(1 - q_B) \log N$  and that of the Alice-Charlie channel is  $(1 - q_C) \log N$ , where, again,  $q_B$  and  $q_C$  are independent of dimension. We see, as before, a  $\log N$  improvement by using qudits. We can also find the capacity of the channel that groups Bob and Charlie together, i.e. Alice is the sender, and Bob and Charlie combined constitute the receiver. We find that the capacity of this channel is  $(1 - q_B q_C) \log N$ . In the case in which Charlie's measurement is optimal, we saw that  $q_B q_C = s$ , so that in that case the channel capacity only depends on the overlap of the initial states.

The situation becomes more complicated when the overlaps, and hence the erasure probabilities, are not the same. As before there are  $N$  inputs  $x \in \{1, 2, \dots, N\}$  and  $N + 1$  outputs,  $y \in \{1, 2, \dots, N, e\}$ . However, we now have that if  $x \in \{1, 2, \dots, M\}$  then the probability that  $y = e$  is  $q_1$  and the probability that  $y = x$  is  $1 - q_1$ . If  $x \in \{M + 1, \dots, N\}$  then the probability that  $y = e$  is  $q_2$  and the probability that  $y = x$  is  $1 - q_2$ . We now need

to calculate the mutual information between Alice and Bob. Setting

$$p_1 = \sum_{x=1}^M P_{in}(x) \quad p_2 = \sum_{x=M+1}^N P_{in}(x), \quad (60)$$

we find that

$$H(Y|X) = p_1 h(q_1) + p_2 h(q_2). \quad (61)$$

The output probability distribution is now

$$P_{out}(y) = \begin{cases} (1-q_1)P_{in}(y) & y \in \{1, 2, \dots, M\} \\ (1-q_2)P_{in}(y) & y \in \{M+1, \dots, N\} \\ p_1 q_1 + p_2 q_2 & y = e. \end{cases} \quad (62)$$

For a fixed value of  $p_1$ ,  $H(Y)$  will be a maximum when  $P_{in}(x) = p_1/M$  for  $x \in \{1, 2, \dots, M\}$  and  $P_{in}(x) = (1-p_1)/(N-M)$  when  $x \in \{M+1, \dots, N\}$ . This gives us that

$$\begin{aligned} I(Y; X) \leq & p_1 q_1 \log \left[ \frac{q_1}{p_1 q_1 + (1-p_1)q_2} \right] \\ & - p_1 (1-q_1) \log \left( \frac{p_1}{M} \right) \\ & + (1-p_1) q_2 \log \left[ \frac{q_2}{p_1 q_1 + (1-p_1)q_2} \right] \\ & - (1-p_1)(1-q_2) \log \left( \frac{1-p_1}{N-M} \right), \end{aligned} \quad (63)$$

and the bound is achievable.

At this point, we need to maximize the right-hand side of the above inequality in order to find the channel capacity, and results of doing so numerically will be presented shortly. We can also get an idea of the behavior of the right-hand side, which we shall denote by  $G$ , near  $q_1 = q_2$  by employing a series expansion. Let  $q_1 = q + \delta q$  and  $q_2 = q - \delta q$ . When  $q_1 = q_2$ , the maximum of  $G$  is obtained when  $p_1 = M/N$  (all inputs equally likely) so we can also set  $p_1 = (M/N) + \delta p$ . Expanding  $G$  up to second order in  $\delta p$  and  $\delta q$ , we obtain

$$\begin{aligned} G = & (1-q) \log N + \delta q \left( 1 - \frac{2M}{N} \right) \log N \\ & + (\delta q)^2 \frac{2M(N-M)}{qN^2 \ln 2} \\ & + 2 \left( \frac{1}{\ln 2} - \log N \right) \delta p \delta q - \frac{(1-q)N^2}{M(N-M) \ln 2} (\delta p)^2. \end{aligned} \quad (64)$$

This can be maximized with respect to  $\delta p$ , and we find

$$G_{max} = (1-q) \log N + \delta q \left( 1 - \frac{2M}{N} \right) \log N + O(\delta q^2). \quad (65)$$

$G_{max}$  is, in fact, the channel capacity. One can check that the above expression is reasonable by noting that if  $\delta q > 0$ , which implies that the states with  $1 \leq j \leq M$

Channel capacity

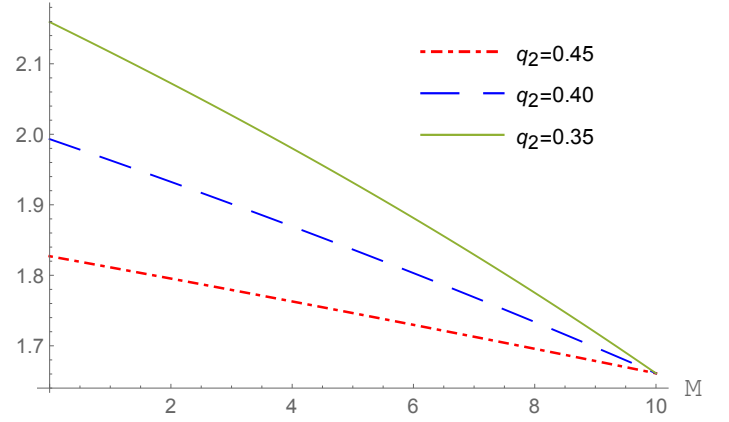


FIG. 1: Channel capacity as a function of  $M$  for  $N = 10$ ,  $q_1 = 0.5$  and three values of  $q_2$ .

Channel capacity

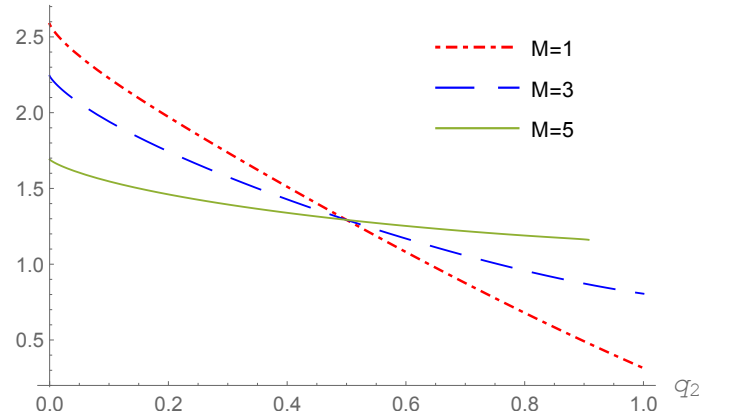


FIG. 2: Channel capacity as a function of  $q_2$  for  $N = 6$ ,  $q_1 = 0.5$ , and three different values of  $M$ .

have a larger failure probability than those with  $M+1 \leq j \leq N$ , then if  $M > N/2$ , the channel capacity is lower than its  $\delta q = 0$  value, because a majority of the states have a higher failure probability.

We supplement this with numerical calculations of the channel capacity. In the first case we examine it as a function of  $q_2$  for a fixed value of  $q_1$  ( $q_1 = 0.5$ ) and different values of  $M$  (see Fig. 1). In the second, we plot it as a function of  $M$  for  $q_1 = 0.5$  and different values of  $q_2$  (see Fig. 2). As expected, the channel capacity is lowest for high values of  $q_2$  and low values of  $M$ .

## V. A SIMPLE EAVESDROPPING ATTACK

The scheme we have proposed, successive unambiguous discrimination measurements on the same qudit, can be useful for constructing a quantum communication protocol that uses nonorthogonal quantum states. We would like now to investigate the robustness of this scheme

against a simple eavesdropping attack, for the equal overlap case, and see how the information gained by the eavesdropper depends on the dimension of the transmitted system. If Eve captures the qudit that was sent to one of the parties, she may choose to apply unambiguous state discrimination to the qudit, but there is a probability that her measurement will fail. If it does, she will have to guess the state that needs to be sent to the next party. This means that she will gain no information about the qudit and will introduce errors. In the case of qubits, a better strategy is for Eve to use minimum-error state discrimination to try to identify the state [11]. Unlike unambiguous discrimination, minimum-error discrimination returns a result every time, but the result can be incorrect. The probability of making an error, however, is minimized.

For symmetric states, the minimum-error measurement is known [12, 13]. The minimum-error POVM elements for the qudit states  $\{|\eta_j\rangle\}$  for  $j = 1, \dots, N$  are given by

$$\Pi_j = \frac{1}{N} \rho^{-1/2} |\eta_j\rangle \langle \eta_j| \rho^{-1/2}, \quad (66)$$

where  $\rho = (1/N) \sum_{j=1}^N |\eta_j\rangle \langle \eta_j|$ . The POVM elements and the success probability for the equal-overlap case were derived by Englert and Řehaček [8]. For the sake of completeness, we work them out in our notation in an appendix. If each state is equally likely, the probability that Eve successfully identifies the state is given by:

$$\begin{aligned} P_{\text{success}}^{(Eve)} &= \frac{1}{N} \sum_{j=1}^N \langle \eta_j | \Pi_j | \eta_j \rangle \\ &= \frac{1}{N^2} \left( \sqrt{1 + (N-1)s} + (N-1)\sqrt{1-s} \right)^2 \end{aligned} \quad (67)$$

Figure 1 shows Eve's success probability as a function of  $s$  for different values of  $N$ . We note that as  $N$  increases, the success probability decreases and approaches  $1-s$  as a limit. Therefore, using qudits rather than qubits, the success probability of someone using a minimum-error strategy to determine the transmitted state is decreased. Assuming that Eve sends a copy of the same state she detects, this would also lead to an increased error probability for the legitimate users. They can detect these by comparing publicly a subset of their results. If there are errors, then an eavesdropper was present.

## VI. CONCLUSION

We have studied a scheme in which successive unambiguous discrimination measurements are made on qudits

in order to determine which state was originally sent. Two different scenarios were studied, the first in which all of the states have the same overlap and the second, in which there are two sets of states, with the states within each set having the same overlap, but the overlaps being different for the two sets. The methods developed

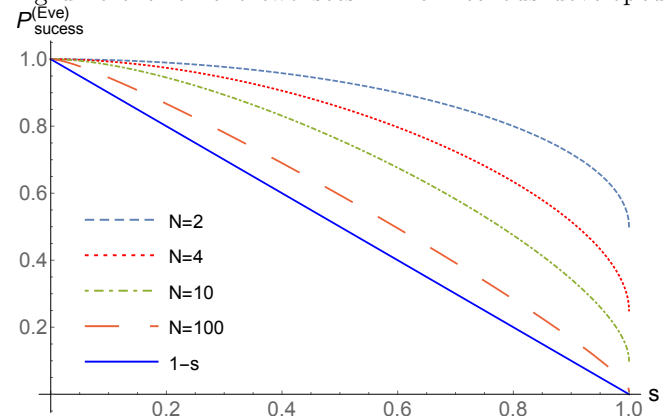


FIG. 3: Eve's success probability as a function of  $s$  for different values of  $N$ . As  $N$  increases, the success probability goes to  $1-s$ .

here can be extended to the case of more sets with different overlaps. The results were compared to those in which qubits are sent in order to determine the effect of using a higher dimensional system. We found that the failure probabilities of the unambiguous discrimination measurements for the case of  $N$  qudits of dimension  $N$  are essentially the same, for the examples we examined, as they are for two qubit states. This means that there is no penalty for using qudits, and therefore, qudits can carry more information per transmission than qubits, and we explicitly calculated channel capacities to show this. We also studied a simple eavesdropping scheme and found that the use of qudits leads to a greater probability of error for the eavesdropper and, thereby, a greater probability that she will introduce errors that will be detected by legitimate users.

## Acknowledgment

MH was supported by a grant from the John Templeton Foundation. JM acknowledges support from a Naval Innovative Science and Engineering (NISE) Basic and Applied Research grant.

[1] P. Rapčan, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, and V. Bužek, Phys. Rev. A **84**, 032326 (2012).

[2] J. Bergou, E. Feldman, and M. Hillery, Phys. Rev. Lett.



- 111**, 100501 (2013).
- [3] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
  - [4] D. Dieks, Phys. Lett. A **126**, 303 (1988).
  - [5] A. Peres, Phys. Lett. A **128**, 19 (1988).
  - [6] For a review of state discrimination see Discrimination of Quantum States by J. A. Bergou, U. Herzog, and M. Hillery in *Quantum State Estimation*, edited by M. G. A. Paris and J. Řehaček (Springer Verlag, Berlin, 2004).
  - [7] A. Chefles and S. Barnett, Phys. Lett. A **250**, 223 (1998).
  - [8] B.- G. Englert and J. Řehaček, J. Mod. Optics **57**, 218 (2010).
  - [9] A. Chefles, Phys. Lett. A **239**, 339 (1998).
  - [10] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, (Wiley, Hoboken, NJ, 2006).
  - [11] J. Bergou and M. Hillery, *Introduction to the Theory of Quantum Information Processing*, (Springer, New York, 2013).
  - [12] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Th. Phys. **36**, 1269 (1997).
  - [13] Y. C. Eldar and G. D. Forney, Jr., IEEE Trans. Inf. Theory **47**, 858 (2001).
  - [14] S. Barnett and S. Croke, Advances in Optics and Photonics **1**, 238 (2009).

## Appendix A

We wish to find the vector  $|\eta_j^\perp\rangle$  that satisfies  $\langle\eta_j^\perp|\eta_k\rangle = 0$  for  $j \neq k$  for the case in which the vectors are divided into two sets, with different overlaps for the different sets. As before we expand  $|\eta_j^\perp\rangle$  in terms of the vectors  $|\eta_k\rangle$

$$|\eta_j^\perp\rangle = \sum_{l=1}^N d_l |\eta_l\rangle, \quad (68)$$

and define the quantities

$$\begin{aligned} \Lambda_1 &= \sum_{l=1}^M d_l \\ \Lambda_2 &= \sum_{l=M+1}^N d_l. \end{aligned} \quad (69)$$

The condition  $\langle\eta_k|\eta_j^\perp\rangle = 0$  for  $k \neq j$  gives us that for  $k \neq j$  and  $k \leq M$ ,

$$d_k = \frac{-1}{1-s_1^2} (s_1^2 \Lambda_1 + s_1 s_2 \Lambda_2), \quad (70)$$

and for  $k \neq j$  and  $k \geq M+1$

$$d_k = \frac{-1}{1-s_2^2} (s_1 s_2 \Lambda_1 + s_2^2 \Lambda_2). \quad (71)$$

In order to find  $d_j$ , we have to consider two cases,  $d_j \leq M$  and  $d_j \geq M+1$ . We will first do the  $j \leq M$  case and give the result for the  $j \geq M+1$  case. Summing the first

if the above equations from 1 to  $M$  and the second from  $M+1$  to  $N$  we find

$$\begin{aligned} \Lambda_1 - d_j &= \frac{-(M-1)}{1-s_1^2} (s_1^2 \Lambda_1 + s_1 s_2 \Lambda_2) \\ \Lambda_2 &= \frac{-(N-M)}{1-s_2^2} (s_1 s_2 \Lambda_1 + s_2^2 \Lambda_2). \end{aligned} \quad (72)$$

These equations allow us to find  $\Lambda_1$  and  $\Lambda_2$  in terms of  $d_j$ , which, in turn, allows us to find  $d_k$  for  $k \neq j$  in terms of  $d_j$ . Defining

$$D_1 = [1 + s_2^2(N-M-1)](1-s_1^2) + (M-1)s_1^2(1-s_2^2), \quad (73)$$

we have that for  $k \neq j$  and  $k \leq M$

$$d_k = \frac{-s_1^2(1-s_2^2)}{D_1} d_j, \quad (74)$$

and for  $k \geq M+1$

$$d_k = \frac{-s_1 s_2(1-s_1^2)}{D_1} d_j \quad (75)$$

The normalization condition on the state then gives us

$$d_j = \left[ \frac{D_1}{(1-s_1^2)(D_1 + s_1^2(1-s_2^2))} \right]^{1/2}. \quad (76)$$

This then gives us that for  $j \leq M$

$$\langle\eta_j|\eta_j^\perp\rangle = \frac{1}{D_1^{1/2}} [(1-s_1^2)(D_1 + s_1^2(1-s_2^2))]^{1/2}. \quad (77)$$

Now let us look at the  $j \geq M+1$  case. Defining

$$D_2 = s_2^2(1-s_1^2)(N-M-1) + (1-s_2^2)[1 + s_1^2(M-1)] \quad (78)$$

we find that for  $k \leq M$

$$d_k = \frac{-s_1 s_2(1-s_2^2)}{D_2} d_j \quad (79)$$

and for  $k \geq M+1$  and  $k \neq j$

$$d_k = \frac{-s_2^2(1-s_2^2)}{D_2} d_j. \quad (80)$$

From this we have that

$$d_j = \left[ \frac{D_2}{(1-s_2^2)(D_2 + s_2^2(1-s_1^2))} \right]^{1/2}. \quad (81)$$

Finally, we find that for  $j \geq M+1$

$$\langle\eta_j|\eta_j^\perp\rangle = \frac{1}{D_2^{1/2}} [(1-s_2^2)(D_2 + s_2^2(1-s_1^2))]^{1/2}. \quad (82)$$

## Appendix B

Here we derive the POVM elements for the minimum-error measurement for the equal-overlap case using our notation. In order to make use of Eq. (66), we have to diagonalize  $\rho$  in order to find  $\rho^{-1/2}$ . The eigenvalue equation  $\rho|\Psi\rangle = \lambda|\Psi\rangle$  implies, if we set  $|\Psi\rangle = \sum_{j=1}^N c_j|\eta_j\rangle$ , that

$$\frac{1}{N} \sum_{j=1}^N [c_j + s(\sum_{k \neq j} c_k)] |\eta_j\rangle = \lambda \sum_{j=1}^N c_j |\eta_j\rangle. \quad (83)$$

Defining  $\Gamma = \sum_{j=1}^N c_j$ , this implies, since the  $|\eta_j\rangle$  are linearly independent,

$$c_j + s(\Gamma - c_j) = Nc_j, \quad (84)$$

or

$$c_j = \frac{s\Gamma}{N\lambda + s - 1}. \quad (85)$$

Summing this over  $j$  we obtain the consistency condition

$$\Gamma = \frac{Ns\Gamma}{N\lambda + s - 1}. \quad (86)$$

There are two cases,  $\Gamma \neq 0$  and  $\Gamma = 0$ . In the first case, we find that all of the  $c_j$ 's are equal, and

$$\lambda = \frac{1}{N}[1 + (N-1)s]. \quad (87)$$

The corresponding normalized eigenvector is

$$|u_1\rangle = \frac{1}{\sqrt{N}[1 + (N-1)s]^{1/2}} \sum_{j=1}^N |\eta_j\rangle. \quad (88)$$

If  $\Gamma = 0$ , then the eigenvalue condition becomes

$$\lambda = \frac{1}{N}(1-s), \quad (89)$$

because at least one of the  $c_j$ 's must be nonzero. This eigenvalue is  $(N-1)$ -fold degenerate. Therefore,

$$\rho = \frac{1}{N}[1 + (N-1)s]|u_1\rangle\langle u_1| + \frac{1}{N}(1-s)(I - |u_1\rangle\langle u_1|), \quad (90)$$

and

$$\begin{aligned} \rho^{-1/2} &= \left[ \frac{N}{1 + (N-1)s} \right]^{1/2} |u_1\rangle\langle u_1| \\ &+ \left( \frac{N}{1-s} \right)^{1/2} (I - |u_1\rangle\langle u_1|). \end{aligned} \quad (91)$$

We find that

$$\begin{aligned} \rho^{-1/2}|\eta_j\rangle &= \left[ 1 - \left( \frac{1 + (N-1)s}{1-s} \right)^{1/2} \right] |u_1\rangle \\ &+ \left( \frac{N}{1-s} \right)^{1/2} |\eta_j\rangle. \end{aligned} \quad (92)$$

The norm of this vector is found to be  $\sqrt{N}$ , so this implies that the vector

$$|\gamma_j\rangle = \frac{1}{\sqrt{N}} \rho^{-1/2} |\eta_j\rangle, \quad (93)$$

is normalized. Furthermore, since  $\Pi_j = |\gamma_j\rangle\langle\gamma_j|$ , the minimum-error measurement is just a projective measurement.